26.10.2023 – 11:45 Uhr

ESET APT Report: EU und Ukraine sind weiterhin Hauptziele für ausländische Cyberkriminelle

Jena (ots) -

Der europäische IT-Sicherheitshersteller ESET hat seinen aktuellen APT Activity Report veröffentlicht. Dieser zeigt eindeutig, dass vor allem die EU, Israel und die Ukraine von Attacken staatlich unterstützter Hackergruppen betroffen sind. Mit ihren Aktionen verfolgen Cyberkriminelle unterschiedliche Ziele: Russische Hacker wollen vor allem die Kriegshandlungen gegen die Ukraine unterstützen. Chinesische Gruppen spionieren insbesondere Regierungsorganisationen und Unternehmen in der EU aus, um an sensible Informationen zu gelangen.

Der Bericht fasst Untersuchungsergebnisse zu Advanced Persistent Threat (APT)-Gruppen von April bis September 2023 zusammen. Der ESET APT Activity Report ist auf dem Security-Blog WeLiveSecurity.de kostenlos verfügbar.

"Organisationen weltweit sind immer häufigeren und ausgefeilteren Angriffen ausgesetzt", fasst Jan-Ian Boutin, Direktor von ESET Threat Research, den Bericht zusammen. "Die anhaltenden Cyberangriffe auf die Ukraine und die Cyberspionage aus China zeigen, dass sich der Cyberraum als Austragungsort staatlicher Interessen etabliert hat. Die hohe Erfolgsquote bei Hacks belegt zudem die große Professionalität und die weitreichenden finanziellen Mittel, auf die diese Gruppen zurückgreifen können."

Russische Hacker nutzen neue Werkzeuge und ändern ihre Taktik

Über anderthalb Jahre nach Kriegsbeginn ist die Ukraine noch immer das Hauptziel russischer Hacker. Sandworm, eine berüchtigte zum russischen Militärgeheimdienst GRU gehörende Hackergruppe, nutzte bei ihren Attacken im April bekannte Malware-Versionen wie "NikoWiper" und "RoarBat", aber es kam mit "SharpNikoWiper" auch eine neue Variante zum Einsatz. Das Ziel der Gruppe ist weiterhin, Daten auf den Computern ihrer Opfer zu löschen und weiter Zerstörungen anzurichten. Hierbei wurden hauptsächlich Behörden und Ämter, aber auch Privatunternehmen und Medienhäuser angegriffen.

Bei anderen Gruppen hat sich das Ziel der Angriffe verschoben: Zu Beginn des Krieges standen Sabotageaktionen im Vordergrund, um Infrastruktur und Verteidigung der Ukraine zu schwächen. Aktuell konzentrieren sich Hacker vermehrt auf Cyberspionage. Die Gamaredon-Gruppe stahl beispielsweise im April Zugangsdaten von Outlook-Konten und Browser-Cookies für sogenanntes Session Hijacking. Darüber hinaus konnte sie mit Hilfe neuer Hacking-Werkzeuge Informationen aus Desktop- und Web-Anwendungen von Telegram, Signal und WhatsApp abgreifen. Mit ihren Aktionen zielten die Kriminellen vor allem auf Chat-Informationen ukrainischer Militärangehörigen ab - womöglich um Kenntnis über Truppenbewegungen, -standorte und -logistik zu erhalten.

Cyberattacken auf Israel

Wie die ESET Forscher zudem herausfanden, operieren Gruppen aus dem Iran und anderen nahöstlichen Ländern weiterhin in großem Umfang. Sie konzentrieren sich bei ihren Aktionen auf Spionage und Datendiebstahl bei Organisationen in Israel. Die mit Iran verbündete Gruppe MuddyWater hatte auch eine nicht identifizierte Einrichtung in Saudi-Arabien im Visier. Die eingesetzte Schadsoftware legt den Schluss nahe, dass dieser Bedrohungsakteur als Wegbereiter für eine fortgeschrittenere Gruppe dient.

China: Zauberer und Goblins & Co. greifen Europa an

Der ESET Activity Report gibt darüber hinaus Einblick in drei neu entdeckte Gruppen, die von China aus Regierungsorganisationen in Europa und Unternehmen weltweit angreifen. DigitalRecyclers ist seit 2018 in der EU aktiv und verteilt über kompromittierte Microsoft Exchange-Server Malware auf die Rechner von Regierungsmitarbeitern. Die Gruppe TheWizards setzt auf Adversary-in-the-Middle-Angriffe, bei denen sich Cyberkriminelle in die Kommunikation fremder Rechnernetze einklinken, um kritische Daten abzugreifen. Zu guter Letzt installierte PerplexedGoblin eine Backdoor namens "TurboSlate" auf den Systemen europäischer, staatlicher Organisationen.

Über den ESET APT Activity Report

Der ESET APT Activity Reporterscheint zweimal im Jahr und fasst die untersuchten Aktivitäten von Advanced Persistent Threats (APT) zusammen. Die aktuelle Ausgabe umfasst den Zeitraum April bis September 2023.

Zeitlich versetzt veröffentlicht der Sicherheitshersteller zudem halbjährliche Threat Reports, die sich mit der allgemeinen Bedrohungslage auseinandersetzen.

Weitere technische Informationen sowie den vollständigen ESET APT Activity Report finden Sie auf WeLiveSecurity.de.

Pressekontakt:

ESET Deutschland GmbH

Christian Lueg
Head of Communication & PR DACH
+49 (0)3641 3114-269
christian.lueg@eset.de

Michael Klatte
PR Manager DACH
+49 (0)3641 3114-257
Michael.klatte@eset.de

Philipp Plum
PR Manager DACH
+49 (0)3641 3114-141
Philipp.plum@eset.de

Folgen Sie ESET:
http://www.ESET.de

ESET Deutschland GmbH, Spitzweidenweg 32, 07743 Jena, Deutschland